IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF	)	**FILED UNDER SEAL**
INFORMATION ASSOCIATED WITH	)	
FOUR (4) APPLE iCLOUD ACCOUNTS	)	Case Nos. 3:23sw 45
DESCRIBED IN ATTACHMENT A	)	3:23sw 46
THAT IS STORED AT PREMISES	)	3:23sw 47
CONTROLLED BY APPLE INC.	)	3:23sw 48

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Douglas H. West, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with Apple iCloud DSID(s) 343894775, 10731117717, 17607233123, and 20724782097 (the "TARGET ACCOUNTS"), which are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. Your affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I have been employed by the Henrico County Police Division as a Police Officer since January 2001. I am currently assigned as a Task Force Officer with the Federal Bureau of Investigation (FBI) where I investigate domestic terrorism matters.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, contraband, instrumentalities, and/or fruits of violations of **Possession of a Destructive Device** (26 U.S.C. § 5861(d)), **Felon in Possession of a Firearm** (18 U.S.C. § 922(g)(1)), and **Interstate Communication of Threats** (18 U.S.C. § 875(c)), as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

RELEVANT STATUTORY PROVISIONS

6. **Possession of a Firearm or Ammunition by a Prohibited Person** (18 U.S.C. § 922(g)(1)). Federal Code prohibits "any person who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year . . . to ship or transport in interstate or foreign commerce, or possess in or affecting commerce, any firearm or ammunition; or to receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce."

7. **Possession of a Destructive Device** (26 U.S.C. § 5861(d)). The National Firearms Act in Federal Code prohibits the receipt, possession, production, or transport of an unregistered "firearm," which § 5845 defines the term "firearm" to include "destructive devices."

8. **Interstate Communications with a Threat to Kidnap or Injure** (18 U.S.C. § 875(c)). Federal Code prohibits the interstate communications of true threats to injure or kidnap any other person.

PROBABLE CAUSE

9. The Federal Bureau of Investigation (FBI) is conducting an investigation into XAVIER LOPEZ, after learning of that individual's social media postings calling for the destruction of Israel and New York City, as well as the deaths of "Jews" and "Yankees."

10. Your affiant learned that LOPEZ was associated with an Instagram account with username "slenderman14w." Your affiant knows through his training and experience that 14w is often used by white supremacists as a reference to "14 words." According to the Anti-Defamation League website adl.org, the phrase "14 Words" is "a reference to the most popular white supremacist slogan in the world: 'We must secure the existence of our people and a future for white children.'" Through open-source search your affiant viewed the publicly visible content on this Instagram page. The content included anti-Semitic memes and white supremacist content. One post declared that "race traitors" are people of European ancestry that fraternize with "blacks," and further, that miscegenation (procreation between individuals of different races) is "race treason," and that race treason is a Capital Offense and will be punished by Death.

11. In August 2020, LOPEZ was arrested for vandalism in Henrico County. Your affiant reviewed video related to this offense and observed LOPEZ, wearing camouflaged pants and carrying a blue flag with a white star, cutting the tires of another person's vehicle. The flag

was identified through open-source searches as a "Bonnie Blue" flag. This flag is associated with the Confederate Army during the United States Civil War. During his arrest and transport to jail, LOPEZ attempted to open a pocketknife. The transporting officer pulled over and removed LOPEZ from the police vehicle. Your affiant reviewed Body Worn Camera footage that showed LOPEZ assault the officer when LOPEZ was taken out of the vehicle. LOPEZ was charged with assaulting law enforcement based on this interaction.

12. As part of a plea agreement, LOPEZ pled guilty to Felony Vandalism. As a convicted felon, LOPEZ was thereafter (and remains) legally prohibited from possessing firearms or ammunition. LOPEZ was ordered to surrender all firearms, ammunition, and firearms components to Henrico Police. In December 2021, a family member turned over LOPEZ's property to Henrico County Police. LOPEZ's property included more than 1,000 rounds of 5.56/.223 ammunition, 15 AR-style magazines with 30 round capacity, two 40 round AR-style magazines, four AR-15 80% lower receivers (also referred to as "80% lowers"), three complete AR-style upper receivers, one jig kit for AR-15 80% lower receivers, four AR-style trigger/handle kits, and four AR-style stocks.

13. Your affiant knows that a lower receiver is an integral portion of a functioning firearm, connecting to the other pieces of a finished firearm and to which the trigger group, upper receiver, and frame are attached. A completed lower receiver is a "firearm" under United States Code, and is required to bear a serial number. An "80% lower" is an unfinished lower receiver. This unfinished receiver does not have certain holes drilled out that would be required to for the firearm to function. As the "80% lower" is not a completed "firearm" for purposes of United States Code, it does not require the background check and traditional requirements for purchasing a working firearm. Your affiant also knows that a "jig kit for AR-15 80% lower" is a device

designed to properly line up the unfinished lower receiver to make the necessary modifications needed to create a completed, functioning firearm.

14. LOPEZ was released from state custody on June 28, 2021. LOPEZ returned to his previous residence at 1419 Fort Hill Drive in Henrico, an 864-square-foot, single-family home. Investigation has confirmed that this residence is assigned Internet Protocol (IP) address 73.12.94.90, which is serviced by the internet services provider Comcast.

15. Your affiant reviewed video taken on July 4, 2021, that showed LOPEZ and another family member inside the Field and Stream store located in Charlottesville, Virginia. This store sells hunting and firearms items. LOPEZ was observed going to the firearms section and stopping several times. LOPEZ can be observed crouching down to look into a glass case with handguns inside. LOPEZ did not purchase any items.

16. In December 2021, an employee of Cabela's was interviewed in relationship to LOPEZ. Cabela's is a hunting equipment and firearms store in Henrico County. The employee recalled LOPEZ being in the store and having a conversation with him about firearms. LOPEZ indicated that he wanted to build a .308 caliber rifle with an 11.5 inch barrel. LOPEZ told the Cabela's employee that he (LOPEZ) wanted to find 168 grain Winchester 308 ammunition to use with that rifle.

17. In October 2022, your affiant learned that several purchases had been made online and that those items were subsequently delivered to 1419 Fort Hill Drive, Henrico (that is, the defendant's residential address). Among these purchases was a "G19 Build Kit" sold by US Patriot Armory. An employee of US Patriot Armory explained that this kit was a complete Glock 19 (9mm semi-automatic pistol) with the exception of the Receiver or Frame. The kit included the slide, barrel, lower parts kit, and magazine. The package was purchased by the billing name of

"John Jackson," utilizing IP Address 73.12.94.90. The package was delivered on September 1, 2022, and signed for by an individual at LOPEZ's residence. The phone number associated with the order was (304) 427-7732. Similar to the "80% lower" recovered from LOPEZ in the past, your affiant knows that unfinished Glock receivers and jig kits are available for purchase online. As the lower receiver is not fully completed, it does not require the traditional background checks and requirements needed to legally purchase a working firearm.

18. On November 25, 2019, LOPEZ was identified through open-source investigation as using Gab account "@XLliving." LOPEZ utilized his photo on this profile and had provided a username of Xavier Large Lexington. LOPEZ's Gab account was open to the public and your affiant has reviewed posts by LOPEZ that advocate for (*inter alia*) the use of violence with firearms. Representative posts on the account include:

a. "If the path to freedom cannot be cleared by words alone, it must be paved with the blood of those who obstruct it. This is the word of the Lord."

b. "there's no real IQ in communists, as communism is a disease. They aren't people, they're remnants of people who were infected and in becoming infected stopped believing in human rights. Since they no longer believe in human rights, they're forfeiting their status as humans. This means that the communists are real life zombies. The only cure is eradication, for all else has failed. The best implementation of the cure can be found in the form of capsules of lead and copper applied at high speed."

c. "maybe we should start an armed insurrection against the commie scum. Pacifism isn't working, we need war to end all communist presence. Eradicate the disease,

don't reason with it. Violence is a last resort but a resort nonetheless, too much peace has us forgetting that very important fact."

19. Your affiant reviewed records from Gab.com for user name "Cru54d3r." This account was associated with IP address 73.12.94.90 and the email address thirdpositioncrusader@protonmail.com. Public posts and comments posted by "Cru54d3r" included highly anti-Semitic, white supremacist, and racist content similar to previous social media accounts believed to be associated with LOPEZ during this investigation. The profile picture for the "Cru54d3r" Gab account includes an image of the Bonnie Blue flag along with a Confederate flag with a Swastika in the middle. The Bonnie Blue flag, as described above, was the flag LOPEZ was filmed carrying while committing vandalism in August 2020.

20. Among the content posted by "Cru54d3r" were links to video tutorials on how to use a 3D printer to print lower receivers for handguns. Other posts by "Cru54d3r" advocated for firearm possession by convicted felons; the collection and possession of various types of ammunition; the purchase of firearm parts kits through the use of pseudonyms; the use of firearms to kill or injure law enforcement; and the manufacture of homemade explosive devices. Gab posts made by "Cru54d3r" include, e.g.:

a. "All real weapons should be built, not bought, this can be done with a 3D printer and a parts kit, both of which can quite easily be bought untraceably, especially if everyone in the group holds mail for each other, and any debit gift cards used are purchased with cash and registered under a pseudonym when necessary, ammo and magazines should be standardized for each type (carbines being .223/5.56 and STANAG mag compatible, shotguns being .12 gauge, handguns being 9mm and Glock mag compatible, etc.)…"

b. "@Lilr and no, being a convicted felon is not at all a valid excuse for remaining unarmed, stay strapped or get clapped. If you don't have a gun yet, at least acquire the means to make one, parts kits are everywhere and 3d printers are pretty cheap now too. You can also have a decent side hustle selling your builds to our white brothers across the pond and all around the world for monero over TOR or isp."

c. "… have absolutely zero regard for the "law and order" of the kike system that hates you…"

d. "@541er now is the time. Or whenever you decide to act. Nobody's going to be a hero. It's up to you. And me. And every other Fascist Revolutionary to take matters into our own hands. Whatever action you are able to do and get away with. Just do it. Be smart and plan it out. Set a date. Slowly and methodically select your target and gather the necessary info and supplies. War is an art. Become the artist. Your target is your canvas. The blood you will spill and shed in your act is the paint, your action is the brush. Make a masterpiece. Select your target wisely and learn from the mistakes of your predecessors. Ensure that no matter what it hurts the kike system more than the cause. Brevik[1] was the best example of this thus far, but we can do even better…."

---

[1] Anders Behring Brevik is a Norwegian citizen convicted of killing more than 70 people on July 22, 2011 in two separate incidents involving Brevik's use of both explosives and firearms. Brevik explained that his decision to conduct this mass killing was motivated by his fervent belief in far-right ideologies.

e. "… learn how to pick and bypass locks in order to covertly enter into the places necessary to get what you need and/or accomplish any objective you set for yourself…"

f. " . . . Have no tolerance for cops. If they come to your house, that's your cue to shoot them. If you see cops at your white neighbor's house, that's also your cue to shoot them."

g. " . . . Manufacture pipe bombs using match heads or mix acetone and either 35% peroxide or Styrofoam if necessary to manufacture what you need in order to defend yourself against the niggers or police…"

21. As noted above, records from Comcast, Inc. reflect that IP address 73.12.94.90 is associated with internet service provided to 1419 Fort Hill Drive, the residence of Xavier LOPEZ and one other family member. LOPEZ has been interviewed by FBI personnel inside this residence and has been observed entering and exiting the residence on numerous occasions.

22. On November 13, 2022, law enforcement officers executed a state search warrant at LOPEZ's residence at 1419 Fort Hill Drive. Among the items recovered during the search of that residence were a 3D printer, firearm components, a G19 build kit, 6 smoke bombs, 1 smoke grenade, smokeless powder, 9mm ammunition, 8 devices that appear to your affiant to be Molotov cocktails or similar destructive devices, stormproof matches, a 3D printed handgun frame, rifle sling, and assorted rifle parts.

23. An Apple MacBook Pro model A2338 with serial number FVFGD1SSQ05G was also recovered inside LOPEZ's residence on November 13, 2022. Following LOPEZ's arrest, after having been provided with a *Miranda* warning, LOPEZ made a statement to law enforcement

claiming ownership of this laptop. LOPEZ refused, however, to provide the password to unlock the device.

24. During a separate interview with law enforcement, LOPEZ responded to a question about which sources of information inspired his ideology by referencing internet searches and materials available online.

25. LOPEZ has denied ownership of a cell phone, and investigators did not recover a phone believed to belong to LOPEZ during the search of LOPEZ's residence. Interviews of known associates of LOPEZ, as well as other information gathered during the investigation, have corroborated LOPEZ's claim. LOPEZ stated to law enforcement that he used his laptop to communicate with others, a statement subsequently corroborated by an associate of LOPEZ, who confirmed to investigators that he (the associate) understood LOPEZ to be communicating with the associate via a communications application on LOPEZ's laptop computer.

26. Throughout the course of the investigation, investigators have learned—as further noted above and below—that LOPEZ has regularly and repeatedly registered and/or employed shadow social media accounts, electronic messaging accounts, and email addresses utilizing various aliases and other fictitious information (such as email addresses and phone numbers); likewise, LOPEZ has conducted financial transactions (such as the online firearm component purchase described above) using aliases.

27. Your affiant accordingly believes that LOPEZ has likely utilized the Apple laptop in question (while employing such aliases and shadow accounts) to communicate with other individuals known and unknown; to register and utilize communication and social media accounts; to research and order various items online for shipment to LOPEZ's residence; and to research and review materials associated with LOPEZ's extremist ideology. In the process of completing these

various activities on his Apple laptop, your affiant believes LOPEZ would almost certainly have utilized Apple's iCloud services.

28. In January of 2023, your affiant reviewed data provided by Apple pursuant to legal process. That information indicated that Xavier LOPEZ is associated with each of the following Apple accounts (that is, the TARGET ACCOUNTS), as further detailed below:

a. **DSID 20724782097**.

i. Through the course of investigation, the phone number (804) 869-1292 was identified as being used by both LOPEZ and Bernadette HAXHAJ, the individual with whom LOPEZ resided at the Fort Hill residence. LOPEZ utilized this phone number to contact LOPEZ's state probation officer.

ii. Apple records indicate phone number (804) 869-1292 was associated with the email address newspace422@gmail.com. Apple records indicate that this email address is associated with the Apple account DSID: 20724782097, and that account used iCloud features including iCloud backup, Contacts, iCloud Photos, notes, and others.

iii. This Apple account was created on July 21, 2022 from the IP address 73.12.94.90 – that is, the IP address assigned to LOPEZ's residence.

b. **DSID 17607233123**.

i. Through the course of investigation, a phone number of (313) 286-2020 was identified as being used by LOPEZ. Communications service for this phone number was provided by the communications application TextNow. TextNow records show the IP address used to set up this phone number was

73.12.94.90 (that is, the IP address assigned to LOPEZ's residence). Additional records for this phone number reflect regular communication with known associates of Xavier LOPEZ.

ii. Apple records indicate phone number (313) 286-2020 was associated with email address rhodie28@icloud.com. Rhodie28@icloud.com is associated with the Apple account DSID: 17607233123, and that this account used iCloud features including iCloud photos, iCloud drive, notes, mail, and others. This Apple account was created on October 30, 2021, also from IP address 73.12.94.90.

iii. Subscriber information provided by Apple for iCloud DSID: 17607233123 lists subscriber name as "Ian Smith," purportedly residing in Argentina. The Verified phone number is listed as (804) 869-1292, with the provided "Day" phone number listed as (313) 286-2020 (that is, one of the TextNow numbers associated with LOPEZ). Investigators believe that LOPEZ entered "Ian Smith" (and "Smith's" residence as Argentina) as an alias in an attempt to distance himself from the account—based on other evidence tying LOPEZ to the account; LOPEZ's practice of relying upon aliases and shadow communications and social media accounts; and LOPEZ's apparent affinity for Argentina (through the course of investigation, social media accounts associated with LOPEZ, including Instagram account "slenderman14w," have referenced Argentinian leader Juan Peron).

iv. During the investigation, LOPEZ used a variety of aliases to make online purchases of lock picking and lock bypass equipment. In multiple online

orders placed to Sparrows Lockpicks, phone number (313) 286-2020 was entered as contact information. The items purchased were shipped (as directed in the orders) to LOPEZ's residence 1419 Fort Hill Drive. Numerous of these lock picking-type items were recovered by law enforcement inside LOPEZ's bedroom during the search of LOPEZ's residence in November 2022.

c. **DSID 10731117717**.

i. Open source investigative searches confirm that the email address xllopez92@gmail.com was used to create (*inter alia*) an Apple account, a LinkedIn account with the display name "Xavier LOPEZ," and a Gab social media account.

ii. Apple records show iCloud account DSID: 10731117717 was associated with xllopez92@gmail.com. The subscriber name for DSID: 10731117717 is Xavier LOPEZ.

iii. Further, records obtained from PayPal, Inc. pursuant to legal process have identified a Paypal account associated with the email address xllopez92@gmail.com. Paypal subscriber information identifies the user name for this account as Xavier LOPEZ, with a provided date of birth that does, in fact, match LOPEZ's date of birth.

d. **DSID 343894775**.

i. Open source investigative searches confirm that email address mrdaredevil@hotmail.com was used to create a variety of social media accounts, to include an Amazon account, an Apple account, and a Skype

account with the display name "X L." Amazon records identified the subscriber for the account associated with mrdaredevil@hotmail.com as Xavier LOPEZ.

ii. Apple records show iCloud account DSID: 343894775 was associated with mrdaredevil@hotmail.com and that this account used iCloud features including safari browsing history, iCloud drive, contacts, and other features.

iii. Subscriber information for iCloud DSID: 343894775 lists the subscriber name as Xavier LOPEZ, with a subscriber address of 33 Sequoia Drive, Coram, New York 11727. Your affiant knows that in 2020 LOPEZ was in the process of attempting to enlist in the United States Army National Guard. Paperwork submitted by LOPEZ identified LOPEZ's father and mother, and provided addresses for both of those individuals as 33 Sequoia Drive, Coram, New York.

INFORMATION REGARDING APPLE ID AND iCLOUD[2]

29. Apple is a U.S.-based company that produces, among other products, the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

30. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

31. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

32. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

33. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on

Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

34. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

35. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications

between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

36. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

37. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

38. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience,

instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

39. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

40. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

41. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation, including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

42. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

43. Based on the forgoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

45. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Douglas H West

Douglas H. West
Task Force Officer
Federal Bureau of Investigation

Subscribed and attested to me by the affiant in accordance with the requirements of Fed. R. Crim. Pro. 4.1 by telephone this 6th day of March 2023.

/s/ MRC

Hon. Mark R. Colombell
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information and documentation associated with the following Apple iCloud DSID(s) (collectively, the "TARGET ACCOUNTS"):

- 343894775
- 10731117717
- 17607233123
- 20724782097

This information is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), a company headquartered 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the TARGET ACCOUNTS, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which each account was created, the length of service, the IP address used to register each account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the TARGET ACCOUNTS (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network

Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all iCloud Drive data associated with the TARGET ACCOUNTS from January 1, 2022, to present;

d. The contents of all Calendar data associated with the TARGET ACCOUNTS from January 1, 2022, to present;

e. The contents of all Contacts data associated with the TARGET ACCOUNTS from January 1, 2022, to present;

f. The contents of all iCloud Photos data associated with the TARGET ACCOUNTS from January 1, 2022, to present;

g. Any data regarding device backups from January 1, 2022, to present;

h. The contents of all emails associated with the TARGET ACCOUNTS from January 1, 2022 until present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

i. The contents of all non-email messages associated with the TARGET ACCOUNTS from January 1, 2022, until present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the TARGET ACCOUNT (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender

and the recipient of each instant message, and the media, if any, attached to each instant message;

j. All activity, connection, and transactional logs for the TARGET ACCOUNTS (with associated IP addresses including source port numbers), including call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

k. All records and information regarding locations where the TARGET ACCOUNTS or devices associated with the TARGET ACCOUNTS were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

l. All records pertaining to the types of services used;

m. All records pertaining to communications between Apple and any person regarding the TARGET ACCOUNTS, including contacts with support services and records of actions taken; and

n. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

o. All decryption keys associated with FileVault for MacOS devices associated with the referenced TARGET ACCOUNTS stored in the iCloud account.

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of **Possession of a Destructive Device** (26 U.S.C. § 5861(d)), **Felon in Possession of a Firearm** (18 U.S.C. § 922G), and **Interstate Communication of Threats** (18 U.S.C. § 875(c)), and/or his co-conspirators, including for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the TARGET ACCOUNTS, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the TARGET ACCOUNTS were accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the user's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **APPLE INC.**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **APPLE INC.** The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **APPLE INC.**, and they were made by **APPLE INC.** as a regular practice; and

b. such records were generated by **APPLE INC.** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **APPLE INC.** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **APPLE INC.**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature